

The Akenti Access Control System: Use-Condition Generation and Signing Certificate Generation¹

(An Application of Public-key Infrastructure and Digitally Signed Certificates)

William E. Johnston², Srilekha Mudumbai, Mary Thompson
Information and Computing Sciences Division
Ernest Orlando Lawrence Berkeley National Laboratory
University of California



1. This work is supported by the Director, Office of Energy Research, Office of Computation and Technology Research, Mathematical, Information, and Computational Sciences Division, of the U. S. Department of Energy under Contract No. DE-AC03-76SF00098 with the University of California

2. wejohnston@lbl.gov, 510-486-5014, mudumbai@george.lbl.gov, mrt@george.lbl.gov - <http://www-itg.lbl.gov>

The Use-Condition Certificate Generation Process

A resource stakeholder (e.g. data “owner”) will impose use-conditions that must be met before access is allowed. Akenti provides several forms of use-conditions. Example use-conditions:

- ◆ **Some component of an X.509 certificate (e.g. “organization” - fairly general or “common name” - very specific)
(in this case the X.509 certificate supplies all of the required attributes)**
- ◆ **Group membership
(stakeholders can establish their own groups, and attribute certificates issued by parties named by the stakeholder will place a user into the group - i.e., an attribute certificate issued to a user that attests to membership in the group)**



Akenti: Use-Condition Generation

An example use-condition certificate:

-----BEGIN TEXT CERTIFICATE-----

-----BEGIN TEXT-----

use-condition

certificate type

issuerAndCA "/C=US/O=Lawrence Berkeley National

Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National

Laboratory/OU=ICSD/CN=William E. Johnston sg1"

issuer of this cert

resource <http://imglib.lbl.gov/shared/wej>

name of the resource

attribute "(group : HPSS)"

required attribute

scope sub-tree

scope of the access permission

enable access read,write,modify,chmod

permitted actions

subjectCA"/C=US/O=LawrenceBerkeleyNationalLaboratory/OU=ICSD/CN=IDCG-CA"

CA required for user

attributeIssuerAndCA group Attribute "/C=US/O=Lawrence Berkeley National

Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National

Laboratory/OU=ICSD/CN=William E. Johnston sg1" *name and naming authority*

attributeIssuerAndCA group Attribute "/C=US/O=Lawrence Berkeley National

Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National

Laboratory/OU=ICSD/CN=Mary R. Thompson sa2"

-----END TEXT-----

-----BEGIN SIGNATURE-----



Akenti: Use-Condition Generation

0llsQ53O94OPX1/+dv8IwjQxf6MVntZRxeduGWsvaJSnP2RpHTgsYXayln5EFILa

-----END SIGNATURE-----

-----END TEXT CERTIFICATE-----

6 7 8 9 10 11 12



Akenti: Use-Condition Generation



- ◆ By naming the resource, the use-condition issuers (stakeholders) are identified (the *.htauthority* file for the resource is retrieved)
- ◆ Authority scoping is dependent on the nature of the resource policy model. For Web servers, scoping may be established by the location of the stakeholder in the directory hierarchy as illustrated in figures 4 and 5.

Akenti: Use-Condition Generation

The screenshot displays the 'USE CONDITION CERTIFICATE GENERATOR' interface, which is divided into three main sections:

- Top Section:** A window titled 'USE CONDITION CERTIFICATE GENERATOR' with a 'Help' button and a text input field labeled 'Resource'. The input field contains the URL 'http://www-itg.lbl.gov/Akenti.test.we'. A 'Cancel' button is located at the bottom right.
- Middle Section:** A window titled 'Choose Use Condition Issuer and its CA' with a 'Help' button. It features two dropdown menus: 'William E. Johnston sg1' (labeled '(Your Signing Authority)') and 'IDCG-CA' (labeled '(Your Certificate Authority)'). Navigation buttons at the bottom include 'Cancel', '< Back', and 'Next >'.
- Bottom Section:** A window titled 'Validate Use Condition Issuer' with a 'Help' button. It contains two input fields: 'Signing Authority:' with the value 'William E. Johnston sg1' and 'Passphrase :' with the value '*****'. Below these fields is the text '(Passphrase this key was encrypted with)'. At the bottom are 'SUBMIT' and 'CANCEL' buttons.

- ◆ Pick the stakeholder persona that will issue this use condition and unlock the signing key

Akenti: Use-Condition Generation

EXPRESSION BUILDER

Build Expressions and choose Attribute Issuer and its CA

Select Attribute

Help

o
ou
group
cn

Select Attribute Value

Mary R. Thompson
William E. Johnston - maat.lb
Srilekha S. Mudumbai - sandy
William E. Johnston u1

Select Attribute Verifier

IDCG-CA

Verifier

IDCG-CA

☐ (☐ AND ☐ OR ☐ ADD ATTRIBUTE/VALUE PAIR ☐)

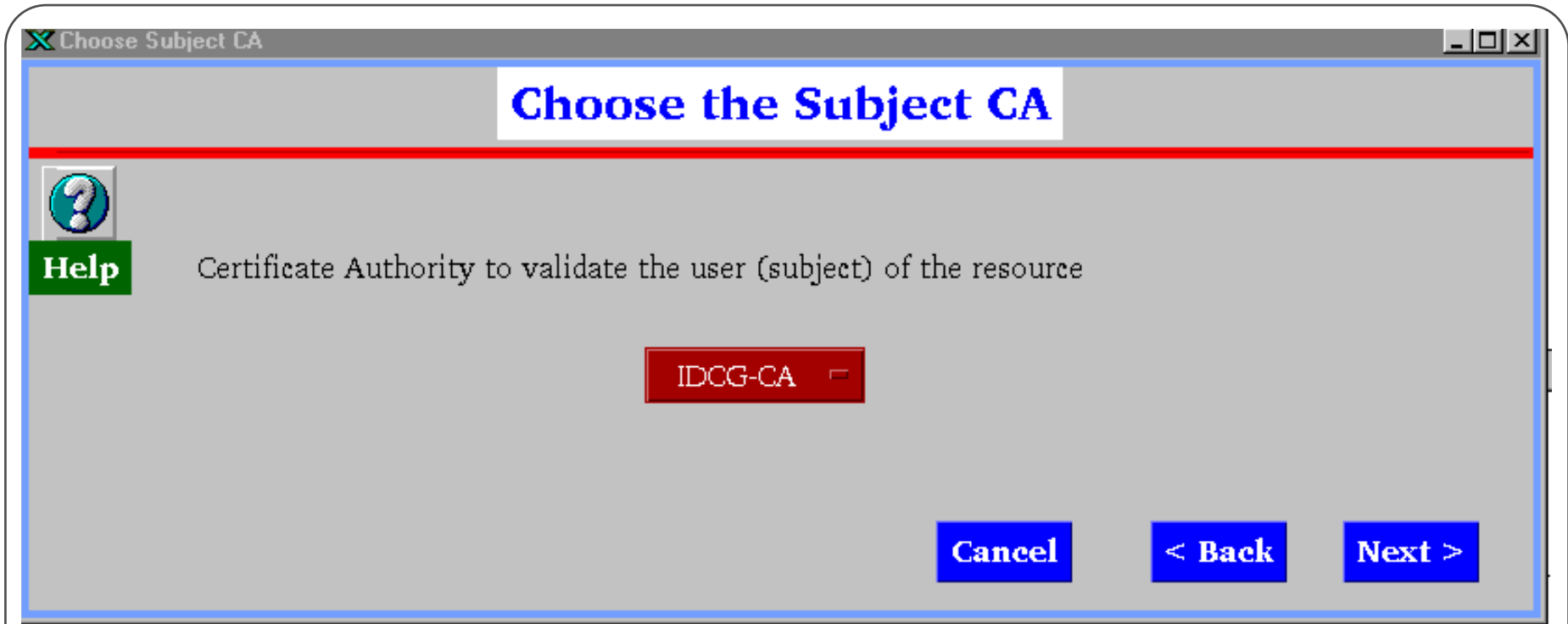
Building Expression

cn = William E. Johnston u1 and cn = Srilekha S. Mudumbai - sandy1@lbl.gov

Cancel < Back Next >

- ◆ The use-condition certificate specifies required attributes and values, together with who is trusted to attest to those attributes.
- ◆ Attributes may be arbitrary name-value pairs, or a component of an X.509 Distinguished Name.

Akenti: Use-Condition Generation



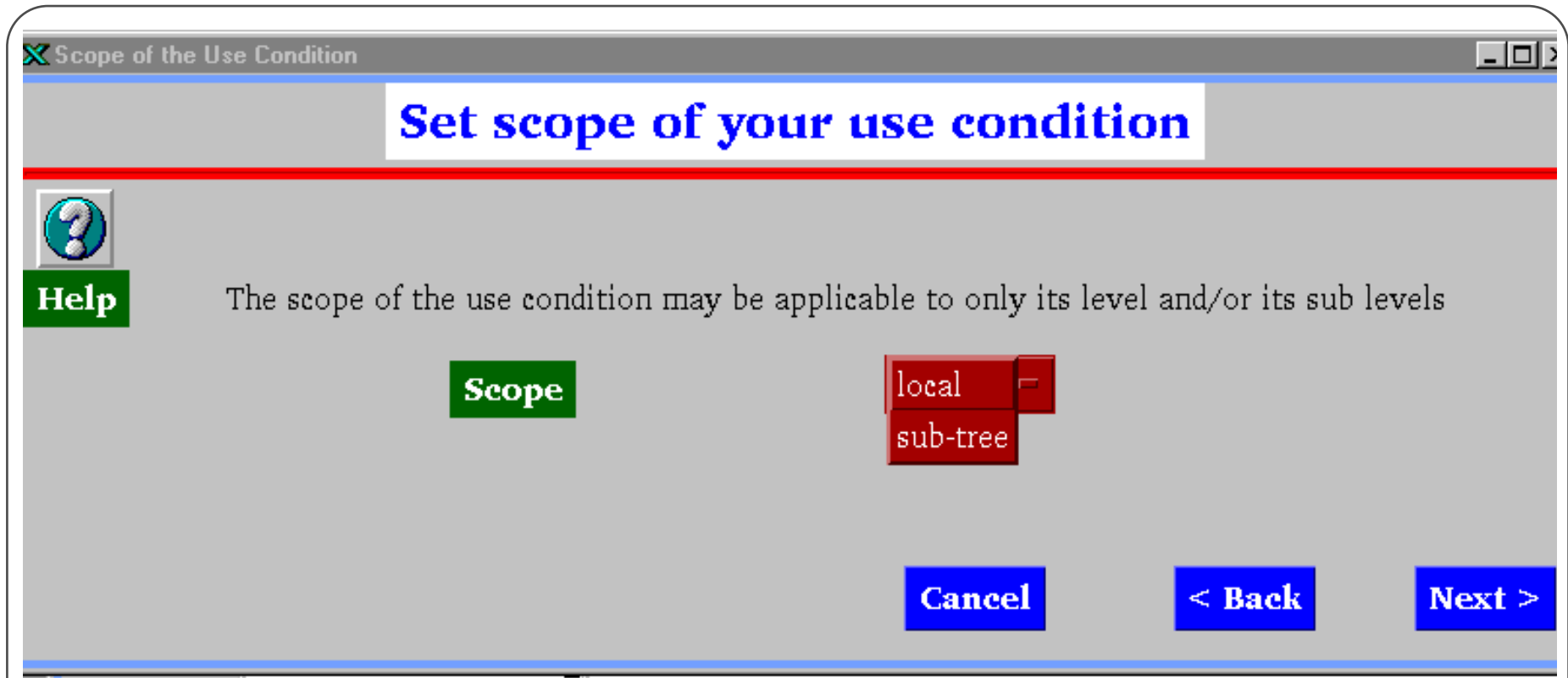
- ◆ If the required attribute is from an X.509 certificate, then the CA of the user that issued the identity certificate must be identified
- ◆ If the required attribute is defined by the stakeholder, then the identity verifier of the user must be separately specified.

Akenti: Use-Condition Generation

The screenshot shows a dialog box titled "Enable Access/Actions". It has a red header bar. On the left, there is a "Help" button with a question mark icon. The main text area contains the instruction: "If access is checked, then all users must satisfy this use condition. otherwise, the use conditions apply only to these actions chosen." Below this text are three buttons: "Enable" (green), "Access" (pink, with a small square icon), and "Actions" (green). The "Actions" button is highlighted, and a blue box next to it lists the actions: "read", "write", and "modify". At the bottom right, there are three buttons: "Cancel", "< Back", and "Next >".

- ◆ In addition to undifferentiated access rights, the use-condition certificate can encode qualifications on actions. The policy engine extracts the permitted “actions” for the target resource as uninterpreted keywords and passes them to the resource server where the action keywords are associated with methods that act on the resource.

Akenti: Use-Condition Generation



- ◆ For resources with a hierarchical policy model, the scope of the use-condition certificate must be specified.

Akenti: Use-Condition Generation

Review Use Conditions Set

IF <expression> THEN <action(s)> WITH <scope>

IF cn = William E. Johnston u1 and cn = Srilekha S. Mudumbai - sandy1@lbl.gov

Attributes, Attribute Certificate Issuers and their CAs

Subject CA Laboratory/OU=ICSD/CN=IDCG-CA

Use Condition Issuer =ICSD/CN=William E. Johnston sg

Use Condition Issuer's CA Laboratory/OU=ICSD/CN=IDCG-CA

Add more Conditions **Cancel** **< Back** **SIGN**

Directory Service - Save Certificate

Enter path or folder name: /home/itgsrvc/security/src/security/lib/Java/

Filter: [^,]*

Files: Action.sh, ActionCertificate.java, AddDelListDialog.java, Attribute.sh, Attribute.sh.old, AttributeCertificate.gui, AttributeCertificate.java, AttributeCertificate.map

Folders: **, Certs, CVS, Database, java

Enter file name: I

OK **Update** **Cancel**

=IDCG-CA" "/C=US/O=Lawrence Berkeley Nati

iases Preferences Quit

rid.Chapter sysadm session 3DES 9.41 12

mmmit Search... More...

ilable in Internet S s Day but *****SUNSO yet recei signed it x version

mpression 3DES 14.31

- ◆ Finally, the completed use-condition certificate is signed by the stakeholder and made available by a trusted server.

Generate A Certificate Singer's key-pair and Identity Certificate

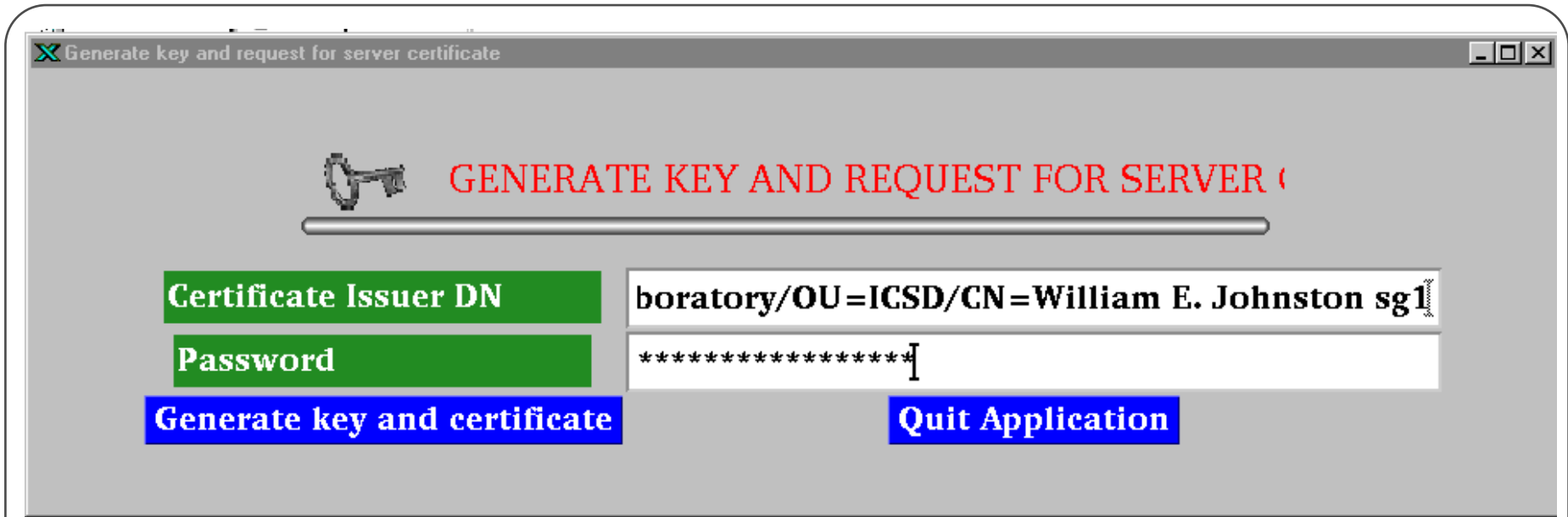
At this point in time, it is not possible to get to the Netscape browser maintained private keys for the purpose of general document signing. Therefore a utility is provided to generate key-pairs for the purpose of Akenti certificate signing. The utility generates an X.509 certificate request in standard format, and this is submitted to the Netscape CA for certification. The CA treats this as a “server certificate” request.

In the future, we may be able to use the Java code signing functions so that the signing certificates may be managed by the browser.


13 14 15



Akenti: Signing Certificate Generation



Generate key and request for server certificate

 GENERATE KEY AND REQUEST FOR SERVER (

Certificate Issuer DN boratory/OU=ICSD/CN=William E. Johnston sg1

Password *****

Generate key and certificate Quit Application

- ◆ Signing key and certificate requests are generated by a program run in the issuer's local environment
- ◆ The encrypted private key and the certificate request are kept in ~issuer/.Akenti
- ◆ Once the certificate for the signing identity is issued, the “identity” is portable - like Netscape v.4 private keys, it may be moved from system to system.



Akenti: Signing Certificate Generation

NETSCAPE CERTIFICATE SERVER

Public Privileged

Public Menu

- [Request a Personal Certificate](#)
- [Request a Server Certificate](#)
- [Search for Certificates](#)
- [List Certificates](#)
- [Accept This Authority in Your Navigator](#)
- [Accept This Authority in Your Server](#)
- [Review Certificate Revocation List](#)

Request a Server Certificate

This form allows you to submit a request to this Certificate Server for a certificate to be used in [another Netscape Server](#). The request should be generated using the administration forms for the other server. In that server's administration forms, visit [Encryption | Request Server Certificate](#).

Server Certificate Request

Cut and paste the [server certificate request](#) into the text area below.

Certificate Request:

```
Data:
  Version: 0 (0x0)
  Subject: C=US, O=Lawrence Berkeley National Laboratory
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public Key: (384 bit)
    Modulus:
      00:d3:b2:5d:e0:1c:ed:d4:fc:a5:12:d6:62:b7
      3b:c0:f5:72:c3:54:af:96:7f:b2:61:40:31:e9
```

Contact Information

Enter information that can be used to reach you regarding this request.

Name: William E. Johnston

E-mail: johnston@george.lbl.gov

Phone: 510-486-5014


Additional Comments To Issuing Agent

Enter any [additional comments](#) directed to the person who will process your certificate request.

Akenti signing certificate request

◆ Any “externally” generated certificate request looks like a “server” request to the Netscape CA interface - this, however, is a signing key request.

Akenti: Signing Certificate Generation



Public Privileged

Public Menu

- [Request a Personal Certificate](#)
- [Request a Server Certificate](#)
- [Search for Certificates](#)
- [List Certificates](#)
- [Accept This Authority in Your Navigator](#)
- [Accept This Authority in Your Server](#)
- [Review Certificate Revocation List](#)

Server Certificate Signing Request

Your request has been submitted and will be processed by a representative of the certificate authority. Please include the reference number below when inquiring about this request. You should save this output until you receive the requested certificate.

Reference Number: 39

Subject Name

CN=William E. Johnston sg2, OU=ICSD, O=Lawrence Berkeley National Laboratory, C=US

Subject Public Key Information

Algorithm: PKCS #1 RSA Encryption
Public Key:
Modulus:
00:d3:b2:5d:e0:1c:ed:d4:fc:a5:12:d6:62:b7:2c:3b:c0:f5:72:c3:54:af:96:
7f:b2:61:40:31:e9:19:d7:8e:b9:96:ff:81:97:a7:99:00:6e:36:c1:ea:8d:8d:
d1:8e:1f
Public Exponent: 65537 (0x10001)

Requestor's Contact Information

Name: William E. Johnston
E-mail: johnston@george.lbl.gov
Phone: 510-486-5014

Requestor's Additional Comments

Akenti signing certificate request

◆ Once the signing certificate is issued and stored in the LDAP database, it is available for validating use-condition certificates

Imaging and Distributed Computing Group,
Information and Computing Sciences Division

15

[Akenti.Use-ConditionCert.process.VG.fm - January 20, 1998]

